CRITICALSTART®

SOLUTION BRIEF

Maximize the value of your SIEM investment.

Achieve the full operating potential of your SIEM.

The strength of your security posture depends on a well-managed SIEM solution. Yet, while SIEM solutions offer many advantages, they can be challenging to deploy, tune and manage, resulting in unused "shelfware" that wastes time and money and creates security awareness gaps. At the same time, the number of people, processes and technology that need constant coordination and monitoring to protect your organization is directly at odds with the increasing demand for simplified cybersecurity that doesn't compromise coverage. Beginning with administering and operationalizing your SIEM, Critical Start resolves these challenges and delivers comprehensive security solutions tailored to your organization's needs.

THE CHALLENGE

A SIEM is not a "set it and forget it" solution. The lack of dedicated resources to tune, configure and test the right log files, etc., is preventing you from getting the greatest security value out of your SIEM. It's also leading to an increase in false positives and alert saturation that clouds decision-making and hides genuine threats. Without complete visibility and control of your data, access to the latest security intel or the ability to scale, your business will continue to struggle to keep ahead of the ever-evolving threat landscape.

The Critical Start solution: Maximizing efficiency without compromising security posture

Critical Start recognizes that your ultimate goal is to ensure effective threat detection and prevention across your organization—and to get there by maximizing your SIEM's performance. ***(Fig 1)*** Because a SIEM is contextual, effective response guidance requires investigation and correlation across multiple security tools. This makes it necessary to:

- ✓ Find and stop threats early in the attack cycle
- ✓ Extend incident response beyond the SIEM
- ✓ Add just-in-time expertise to your team

To address these core challenges, Critical Start offers focused solutions in six specific areas:

1. MIGRATION AND IMPLEMENTATION

A SIEM platform is not a one-off technology purchase—to be successful requires ongoing development and maturation of the SIEM from trained experts. Therefore, we offer assistance with migration from your current SIEM provider(s) and help with implementation.

2. CONFIGURATION

Tuning is critical for achieving the best possible results from your SIEM. We make you more effective with custom configuration, SIEM dashboards, reports and log sources to support your specific security, risk, compliance and audit use cases. This gives you more control over your SIEM data, the use cases it supports and escalation processes and operations.

3. CONTENT

We help you work more efficiently by automating everyday tasks—such as playbook development—and provide expert guidance on how to quickly and effectively respond to incidents using your SIEM data. We design and build detection and reporting content and then translate alerts into information you can do something with.

4. OPERATIONAL MONITORING

With quarterly service reviews, ingest cost analysis and more, we maximize and keep your total cost of ownership predictable and manageable.

CRITICALSTART®

5. TECH MANAGEMENT

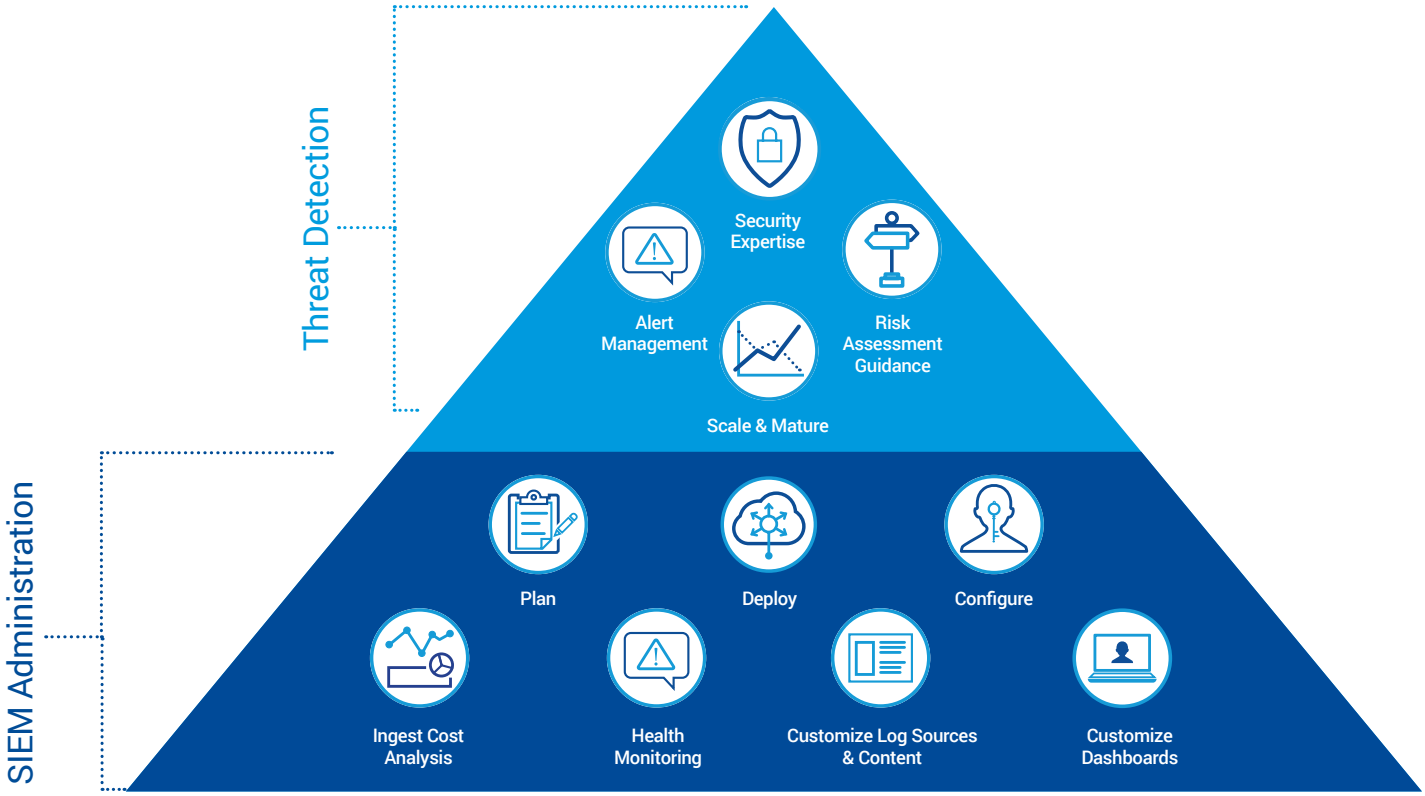
We help simplify resource management and improve team efficiency by staying on top of current changes—even if your SIEM vendor is continuously updating your platform. We make sure your SIEM is up-to-date, address hotfixes and review any out-of-the-box content, allowing your analysts to stay focused on real and emerging threats and help you avoid costly downtime.

6. THREAT MONITORING & INVESTIGATION

Critical Start extends your team with skilled security experts who partner with you to detect, investigate and respond to threats. Our services are powered by the Zero Trust Analytics Platform™ (ZTAP™), 24x7x365 expert security analysts and the Critical Start Cyber Research Unit (CRU). We partner with you to respond to alerts swiftly and effectively, elevating your efficiency level in orders of magnitude greater than can be achieved through manual effort.

CONCLUSION

Using a risk-based approach, Critical Start provides comprehensive services backed by industry-leading methodologies, processes and technologies. By assisting in advancing your cybersecurity capabilities over time (based on your risk profile), we empower organizations like yours to balance cost and risk mitigation to achieve your desired maturity level. We are passionate about our work, committed to your success and proud to provide you with results backed by our one-hour Service Level Agreements (SLAs) for Time to Detection (TTD) and Median Time to Resolution (MTTR) and enhanced by the convenience of our MOBILESOC® app.



(Fig 1) Simplifying breach prevention

KEY OUTCOMES

Maximize the productivity of your team

Our security experts handle the heavy lifting around your SIEM implementation and management. Let us optimize your SIEM with dedicated operational services, including functional updates and version upgrades, so your team can focus on other business priorities.

Optimize financial stewardship & simplify resource management

We help manage your operating costs for SIEM by ensuring you are ingesting the right security data to get the most value from your threat-detection use cases. Critical Start helps you efficiently allocate resources—like understanding what type of log storage is best for your business—which decreases your in-house requirements and results in lower costs for your business.

Quickly access data relevant to your specific use cases

Configure and personalize your SIEM solution with customized SIEM dashboards, reports and log sources to support your specific security, risk, compliance and audit use cases. In addition, you can leverage "single pane of glass" datapoints to prove the value of your SIEM to your executive team.

Enhance your detection coverage & security posture

We map your threat detection content to the industry standard MITRE ATT&CK® Framework and provide the foundation to help you achieve optimal MDR coverage and outcomes. We help you keep up with new threats and compliance requirements by ensuring that your data is being properly ingested, guiding you in applying the right detection content to your log sources and preventing misconfigurations.

KEY SOLUTION FEATURES

Configuration and customization

We configure and customize your dashboards, reports and log sources to support your specific security, risk, compliance and audit use cases.

Quarterly service reviews: Optimizing your detection coverage

Use our in-depth, quarterly report for constant assurance that your log sources coming in are accurate and necessary for detecting threats. Get full visibility into what logs you are ingesting and how your SIEM is performing to help you control costs and increase security outcomes.

(Microsoft Sentinel™ customers receive an ingest cost analysis to analyze billing vs. ingest for specific Microsoft data sources based on your security products and licenses.)

Health monitoring: Keep your SIEM running at optimal capacity

This service offers log source performance, availability and capacity monitoring to identify potential issues with log ingestion.

Risk reduction reviews

If you are thinking about adding more log sources or detection content, we can analyze the potential impact on your coverage under the industry standard MITRE ATT&CK® Framework.

CRITICALSTART®

CRITICALSTART®
They're good. We're better.

For more information about Critical Start services and solutions for Microsoft Security, schedule a demo at:
www.criticalstart.com/contact/request-a-demo/

About Critical Start

Today's enterprise faces radical, ever-growing and ever-sophisticated multi-vector cyber-attacks. Facing this situation is hard, but it doesn't have to be. Critical Start simplifies breach prevention by delivering the most effective managed detection and incident response services powered by the Zero Trust Analytics Platform™ (ZTAP™) with the industry's only Trusted Behavior Registry™ (TBR) and MOBILE**SOC**®. With 24x7x365 expert security analysts and Cyber Research Unit (CRU), we monitor, investigate and remediate alerts swiftly and effectively, via contractual Service Level Agreements (SLAs) for Time to Detection (TTD) and Median Time to Resolution (MTTR) and 100% transparency into our service. For more information, visit criticalstart.com. Follow Critical Start on LinkedIn, Twitter, Facebook, Instagram.

© 2022 CRITICAL**START**. All rights reserved.